



Un white paper a cura di Websense®

Estendi la tua soluzione di sicurezza Web per far fronte alla perdita di dati

Fate evolvere la sicurezza Web

Le tecnologie Web 2.0 stanno trasformando Internet. Quello che, una volta, era poco più di una risorsa di informazioni statiche o quasi, è oggi diventato un canale per comunicazioni altamente dinamiche e una piattaforma più che adatta alle innovative applicazioni di business. I metodi tradizionali per ottenere la sicurezza Web devono trasformarsi di conseguenza, dal momento che le aziende ora richiedono un controllo non solo sulla navigazione Web dei loro utenti, ma anche sugli spostamenti dei loro dati. Una soluzione adeguata permetterà di:

- Favorire lo svolgimento delle attività aziendali autorizzate proteggendo allo stesso tempo utenti e dati;
- Rilevare procedure aziendali sbagliate e agevolare la correzione;
- Raggiungere un obiettivo in tempi rapidi, a vantaggio del team di sicurezza Web. Si accelera infatti la risoluzione di una problematica che sta rapidamente diventando una sfida considerevole per le aziende



Il Web è la nuova piattaforma applicativa

Il Web 2.0 sta Trasformando il Business

Le tecnologie 2.0 hanno irrimediabilmente cambiato la natura del Web e, insieme ad essa, la natura della sicurezza Web. I contenuti Web oggi sono altamente dinamici e hanno aumentato il bisogno di soluzioni di sicurezza capaci di valutazione, categorizzazione e controllo delle minacce in tempo reale. Ma non è tutto. La rivoluzione del Web 2.0 ha anche introdotto l'utilizzo del Web come canale di comunicazioni verso l'esterno. Un aspetto che, grazie alla capacità del Web 2.0 di favorire la collaborazione e facilitare i processi aziendali, è generalmente visto come positivo. Nonostante ciò, c'è un rovescio della medaglia di cui tenere conto: in questo modo aumentano considerevolmente le possibilità che il canale Web diventi una via per l'esposizione involontaria di dati riservati.

Fortunatamente, Websense è in grado di rispondere con una soluzione semplice ma ricca di funzionalità e altamente robusta a questo problema. In particolare, chi utilizza i nostri prodotti per la sicurezza Web può incrementare sostanzialmente il valore di queste soluzioni semplicemente implementando un set completamente integrato di funzionalità senza confronti di Data Loss Prevention (DLP), anch'esso disponibile con Websense.

Web Security:una sfida in evoluzione

Impostare un livello di sicurezza Web adeguato originariamente richiedeva solo un'implementazione di filtraggio URL, integrata da un antivirus e da funzionalità di tutela della Web reputation. Queste tecnologie erano tutte richieste dai dipartimenti IT per contrastare con efficacia l'accesso degli utenti a siti non necessari alla loro attività se non dannosi, fornendo anche protezione in caso di problemi, relativamente rari, con il malware proveniente dal Web.

Tuttavia, il Web 2.0 ha cambiato tutto. Pur consentendo molte funzionalità allettanti in grado di aumentare la comunicazione tra persone e tra aziende, le tecnologie Web 2.0 rendono le cose piuttosto difficili dal punto di vista della sicurezza.

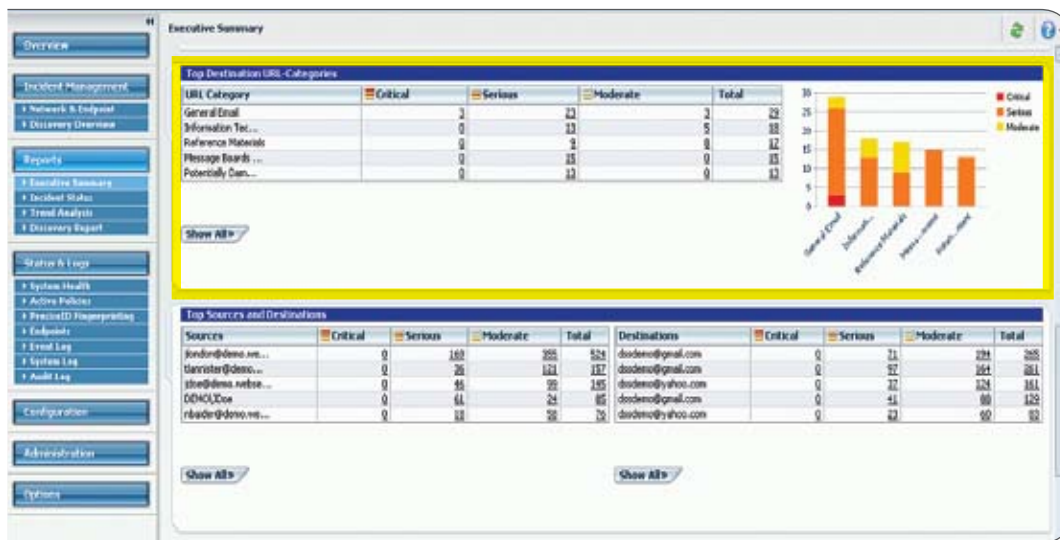
- I siti Web 2.0 sono di gran lunga più complessi e vasti, spesso comprendono milioni di pagine di materiali di tutti i tipi;
- I contenuti Web 2.0 sono particolarmente dinamici, spesso comportano l'attivazione in tempo reale di codice e/o la compilazione di materiale proveniente da più siti diversi; e,
- L'utilizzo diffuso di script e altre forme di codice attivo rendono altamente probabile che anche i siti ritenuti innocui diventino pericolosi.

Come risultato, impostare in modo adeguato la sicurezza Web ora richiede che, oltre alle tecnologie tradizionali che si basano sulla prima identificazione e classificazione di siti, contenuti e minacce associate, debbano essere integrate anche funzionalità di analisi in tempo reale dei contenuti, categorizzazione e controlli di sicurezza.

Ma le organizzazioni non dovrebbero limitarsi a questo. Idealmente, i CIO dovrebbero anche considerare la necessità di incorporare funzionalità di protezione dei dati sensibili alle soluzioni di sicurezza Web a disposizione. Infatti, la potenzialità che il traffico Web diventi un veicolo per la perdita di dati sensibili, involontaria o dolosa, non deve essere sottovalutata. Basti considerare che:

- Un'altra caratteristica significativa delle tecnologie 2.0 è di agevolare la distribuzione di contenuti generati dagli utenti. Questo include la possibilità di pubblicare volontariamente non solo i dati personali, ma anche le informazioni di carattere business.
- Sebbene la posta elettronica abbia costituito l'anello debole in ambito sicurezza dei dati - almeno in termini di quantità di casi di perdita di dati attribuiti storicamente ad essa - non abbiamo assistito ad un particolare cambiamento nel modo in cui questo canale è utilizzato. Per il Web 2.0 è accaduto il contrario: ha profondamente cambiato sia il modo e l'entità con cui il Web è utilizzato, ma ha provocato da subito un considerevole aumento delle possibilità di perdere dati attraverso il Web.
- Per certi versi sembra ironico: queste possibilità potrebbero aumentare con la consumerizzazione dell'IT e con la decisa diffusione del Web 2.0, e delle offerte di Software as a Service (SaaS) strettamente collegate, in risposta ad alcune legittime esigenze aziendali. Questi casi di utilizzo convalidano di fatto il flusso in uscita di dati lungo il Web e, in assenza di una guida o di controlli, possono facilmente condurre gli utenti a credere che sia consentito l'impiego di altri servizi di esportazione/condivisione di dati, in modo particolare se possono essere di aiuto nello svolgimento della loro attività (è il caso di Google Docs, Twitter e LinkedIn).
- Infine, non è solo una questione di contenuti generati dagli utenti e di una crescente massa di codice dannoso proveniente dal web, sviluppato per rubare dati sensibili. A seguito della nascita di siti e strumenti innovativi come Dropbox (www.getdropbox.com), i casi di perdita dei dati attraverso il canale Web sono in crescita anche a causa del fatto che i protocolli Web e i servizi stanno sempre più sostituendo altri metodi tradizionalmente utilizzati per il trasferimento dei dati, come l'FTP e in alcuni casi anche le e-mail (per esempio, quando il peso di un allegato supera i limiti consentiti).

L'impatto di questi cambiamenti, in parole povere, è che il bisogno di proteggere i dati sensibili è di fatto diventato un altro elemento integrante della sicurezza Web, una sfida con cui oggi le aziende devono misurarsi.



È possibile ottenere il contesto della perdita dei dati grazie ai dettagli sull'URL di destinazione

Un problema integrato merita una soluzione integrata

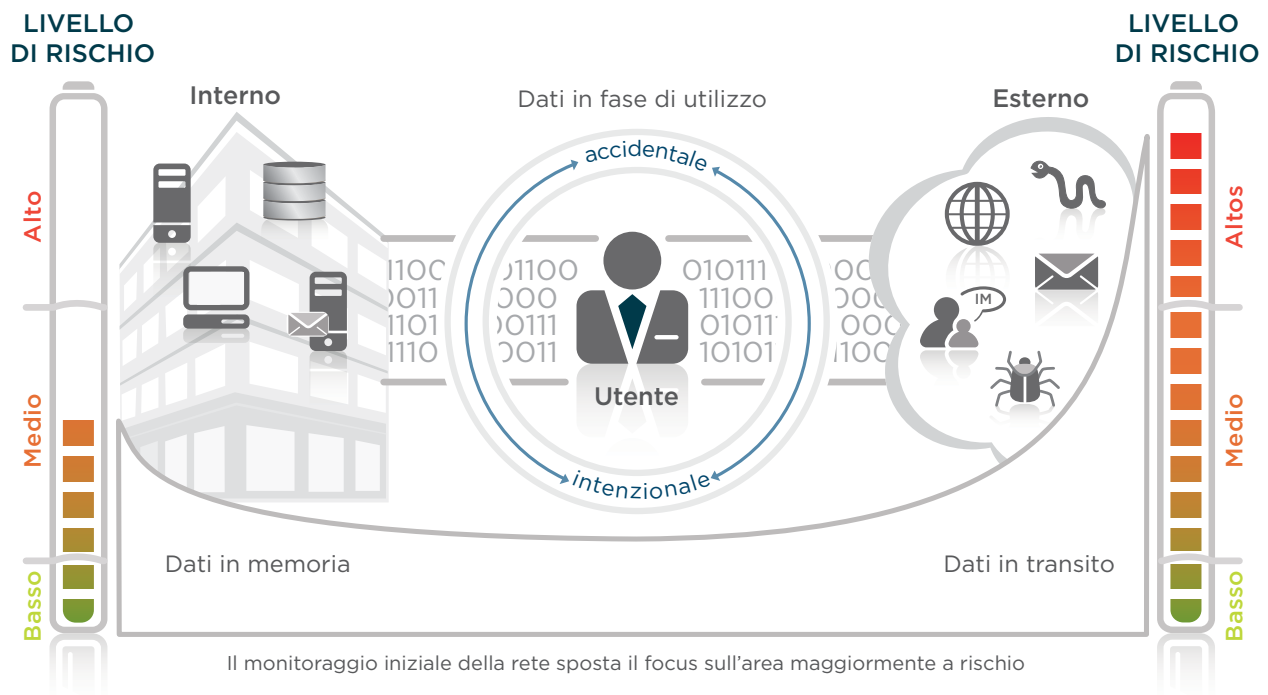
A completamento dell'offerta di un vasto portfolio di soluzioni di sicurezza Web in grado di tenere conto della natura dinamica dei contenuti Web 2.0, Websense mette a disposizione Websense Data Security Suite, una soluzione di DLP leader di mercato. Le funzionalità di cui è dotata possono essere implementate in modalità stand-alone o, aspetto molto conveniente per chi ha già in dotazione altre soluzioni Websense, come estensione integrata dell'infrastruttura di sicurezza Web esistente. Infatti, se si tratta di Websense Web Filter, Websense Web Security, o Websense Web Security Gateway, è possibile sfruttare la stessa soluzione già in uso per controllare "chi va dove" sul Web, gestendo anche "che cosa va dove". In questo modo:

- È possibile ottenere protezione sia per gli utenti che per i dati con una soluzione integrata;
- È possibile impostare e attivare policy di utilizzo autorizzato complete (AUP) per regolamentare lo scambio di dati via web attraverso controlli di policy semplici ma affidabili; e,
- I rischi legati alla produttività, alla responsabilità e alla sicurezza a causa dei contenuti in ingresso, durante la navigazione in Internet, possono essere diminuiti in modo efficiente ed efficace allo stesso modo di quelli dovuti all'esposizione non autorizzata di dati riservati (per esempio, la perdita di vantaggio competitivo e la non conformità con la regolamentazione in vigore).

Ma la capacità di integrarsi con la completa offerta dei prodotti Websense di sicurezza Web costituisce solo un aspetto della forza di questa soluzione. Tra gli ulteriori vantaggi anche la possibilità per le organizzazioni di usare un approccio pratico alla sicurezza dei dati, l'aver a disposizione un set completo e senza confronti di funzionalità e il valore aggiunto che esso consente.

Come attivare un approccio pratico contro la perdita dei dati

Acquistare e implementare una soluzione DPL è una prospettiva che preoccupa molte organizzazioni IT. Ciò deriva da una diffusa convinzione che un'iniziativa in ambito DLP sia un'impresa complicata, in grado di decollare solo dopo aver definito esattamente che cosa i dati sensibili comprendano e quindi a valle di una ricerca completa volta a identificare tutte le ubicazioni in cui essi sono archiviati. Si tratta comunque di un fraintendimento, e, almeno per le soluzioni Websense, non è così. Ha molto più senso, invece, iniziare con il monitoraggio della rete aziendale per ottenere visibilità nel flusso effettivo delle informazioni sensibili e quindi intraprendere le azioni correttive.



Di fatto, ecco i vantaggi di un approccio di questo tipo:

- Le organizzazioni sono in grado di focalizzarsi da subito sui principali rischi. Sia i dati conservati che quelli in utilizzo sui dispositivi degli utenti possono essere soggetti a perdita. Al contrario, nel momento in cui si registra l'uscita di dati dalla rete, per esempio, in un messaggio e-mail, durante la transazione di un'applicazione web o scrivendo su un blog, il rischio diviene reale.
- Costi e sforzi possono essere ridotti. Le organizzazioni non possono perdere tempo discutendo su cosa potrebbe accadere e quali bit o parti di informazioni debbano essere protette. Con il monitoraggio iniziale della rete si ha un quadro completo della situazione, facilitando e accelerando l'identificazione dei dati, la loro classificazione e i processi di sviluppo delle policy necessarie.
- Si può raggiungere l'obiettivo rapidamente. Invece di trascorrere mesi per ottenere risultati significativi, i report possono dimostrare, quotidianamente o mensilmente, la reale portata del problema della perdita dei dati aziendali. Inoltre, è possibile iniziare subito a limitare le fughe. Le sole iniziative dedicate a target specifici, come attestare le policy di utilizzo consentito e l'invio di notifiche e avvisi, ridurranno i casi di perdita dei dati di più del 50%. In tal modo, la credibilità acquisita dovrebbe, come minimo, spianare la strada all'IT per portare a termine il resto delle attività DLP programmate.

Si tratta di vantaggi determinati dal fatto che l'integrazione della sicurezza dei dati con Web Filter e con gli altri nostri prodotti in ambito sicurezza Web, è focalizzata prima di tutto nel consentire ai nostri clienti di controllare e eventualmente proteggersi dall'uscita di dati sensibili dalla loro rete. Questo sistema richiede solo un piccolo investimento per ottenere un ritorno piuttosto vantaggioso.



Calcolo utile della portata dei problemi di perdita dei dati

Un altro punto di forza della soluzione, tuttavia, è che queste funzionalità core sono già di per sé una componente di Websense Data Security Suite. Il che significa che se un'organizzazione decide di farlo, può facilmente estendere la sua implementazione DLP anche ai dati in memoria (per esempio ovunque siano archiviati) e i dati in utilizzo (in qualsiasi momento siano elaborati da un dispositivo di un utente finale).

Websense Data Security Suite

La soluzione Websense Data Security Suite è composta da quattro moduli integrati che possono essere implementati a seconda delle esigenze del cliente:

Websense Data Monitor	Effettua il monitoraggio della rete di chi sta usando quali dati e in che modo
Websense Data Protect	Protegge i dati durante la trasmissione attraverso la rete con controlli basati su policy che mappano i processi aziendali.
Websense Data Endpoint	Estende il monitoraggio e l'applicazione fino al livello di endpoint per proteggere le attività degli utenti
Websense Data Discover	Ricerca e classifica i dati distribuiti in tutta la rete aziendale

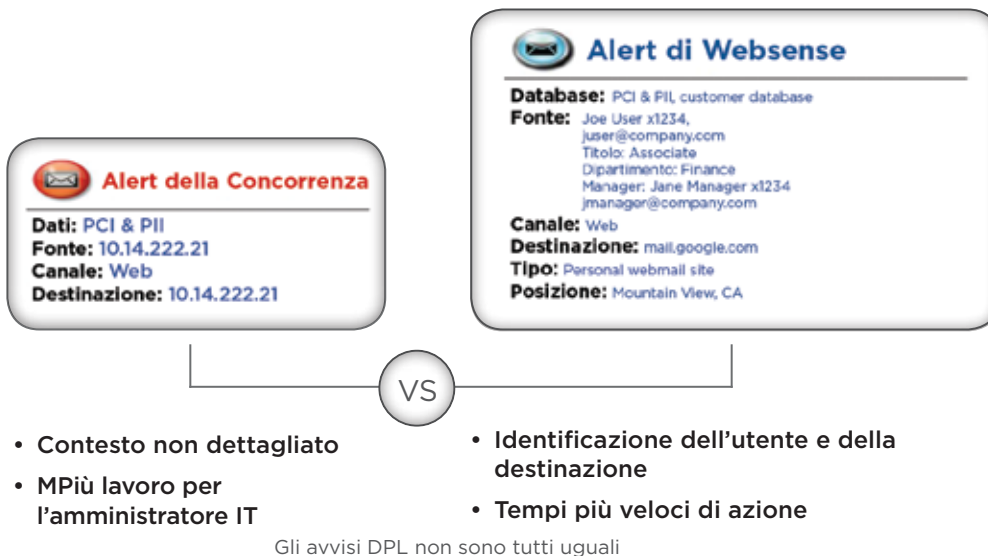
Funzionalità senza confronti

Scendendo nei dettagli, ecco le feature e le caratteristiche specifiche consentite da una sicurezza dei dati integrata. Si tratta di elementi che permettono a chi sceglie le soluzioni Websense, leader di mercato su tutta la linea, di ottenere in modo efficiente ed efficace una conoscenza profonda e un completo controllo dei dati sensibili presenti nella propria rete.

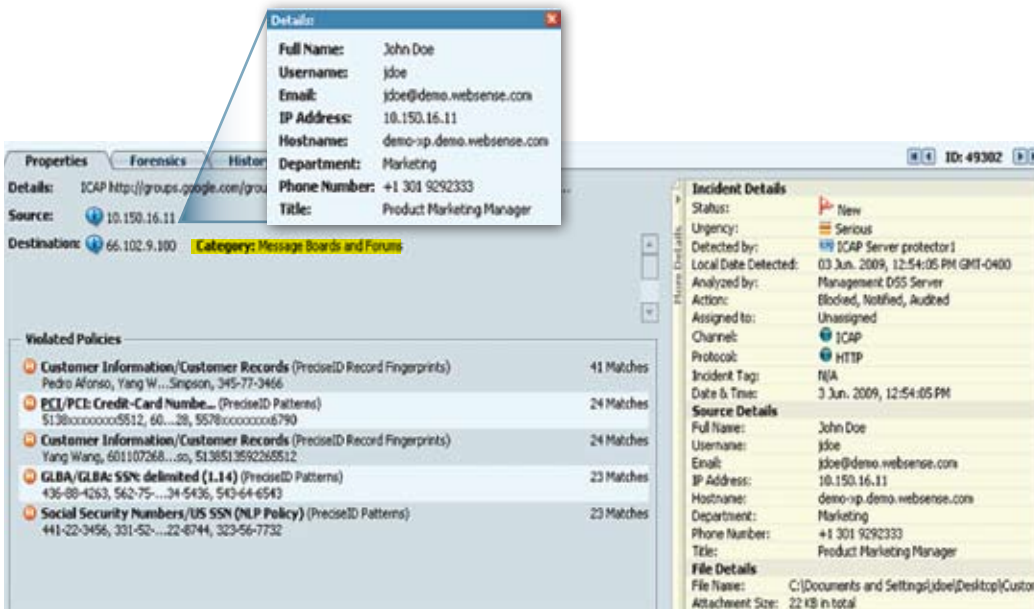
Ampia visibilità

Molte soluzioni si concentrano solo su quali parti di dati si perdono e su come questa perdita si sta manifestando, ovvero attraverso quale particolare protocollo o sistema di comunicazione. Un contesto così ridotto può essere problematico perché spesso genera falsi positivi e limita le applicazioni delle policy e l'accuratezza della reportistica. Al contrario, la soluzione Websense fornisce in aggiunta i dettagli su chi sta inviando i dati e, tramite la funzionalità di identificazione della destinazione in tempo reale, dove nello specifico i dati sono stati inviati. Questi approfondimenti sono ottenibili per i protocolli Web (HTTP), secure Web (HTTPS) e le sessioni dinamiche 2.0.

Consideriamo ora un normale caso di allarme da perdita dei dati in cui sono indicati solo l'indirizzo IP e il canale, lasciando il carico all'amministratore del sistema di determinare a chi occorre inviare la notifica e quali destinazioni specifiche stanno per ricevere i dati.



Messe a confronto, le funzionalità DLP di Websense forniscono una maggiore visibilità e riducono considerevolmente il carico attribuito allo staff IT non solo evidenziando che alcuni dati PCI e PII sono stati persi attraverso il canale Web, ma anche indicando le informazioni sull'identità della persona responsabile del traffico pericoloso e esattamente dove si sta dirigendo.



Gestione dell'incidente grazie alle informazioni su URL e destinazione

Sistema di policy di alto livello

Gli stessi elementi utilizzati per ottenere visibilità sul flusso di dati sensibili (chi, cosa, dove e come) costituiscono la base per un sistema di policy di tipo avanzato utilizzabile per le operazioni di controllo. Attraverso questo sistema, le organizzazioni possono creare policy per i dati che, in modo intelligente e preciso, effettuino una mappatura dei loro specifici processi aziendali. In questo modo le transazioni aziendali autorizzate seguono il loro corso, senza intoppi e in modo granulare. Ma, allo stesso tempo, le attività prive di regolare permesso possono essere sottoposte ad una gamma di provvedimenti come blocco, quarantena, codifica forzata e notifica.



Le aziende possono ottenere visibilità e controllo su chi manda quali dati, dove e in che modo.

Rilevamenti altamente accurati

Il livello di precisione è un requisito fondamentale in una soluzione DLP. Anche una piccola percentuale di falsi positivi può significare centinaia di eventi spuri, ciascuno dei quali in grado di interrompere i processi aziendali e causare costi ingenti, oltre a richiedere l'attenzione dell'amministratore IT e dello staff di helpdesk. Ecco perché Websense integra il consueto set di keyword, dizionari, regular expression, file matching, analisi statistiche e tecniche di correlazione tramite la tecnologia brevettata PreciseIDTM, un innovativo sistema di identificazione in grado di effettuare anche l'elaborazione del linguaggio naturale. La soluzione sfrutta anche i vantaggi di Websense ThreatSeeker™ Network, una raccolta di più di 50 milioni di sistemi che senza interruzione passano in rassegna contenuti Internet per cercare minacce in fase di lancio, e automaticamente forniscono aggiornamenti contestuali a tutti i prodotti di sicurezza e-mail, Web e dati di Websense.

Architettura flessibile

Le caratteristiche di DLP di Websense possono essere utilizzate in modo integrato con qualsiasi altro prodotto di sicurezza Web di Websense, in modalità sia pass-by (porta span) o in linea (proxy tap). In alternativa, possono anche essere configurate per funzionare con un proxy Web standard o con la soluzione Websense Email Security. Le aziende possono ottenere vantaggi sia dalla protezione dell'investimento effettuato, che dalla possibilità di integrare gli altri moduli compresi nella soluzione Websense Data Security Suite, con il sistema di DLP implementato a seconda delle loro esigenze, per esempio per attivare la ricerca e il monitoraggio a livello endpoint e le relative funzionalità di controllo.

Gestione affidabile

La gestione centralizzata è fornita per tutte le funzioni del ciclo di vita. La configurazione delle policy è facilitata da procedure guidate integrate e da una raccolta completa di template, aggiornati da Websense, a copertura della lista completa delle normative del settore (per esempio PCI, GLBA, HIPAA e SOX), e le diverse categorie di informazioni sensibili, come PII (personally identifiable information), PHI (personal healthcare information) e PFI (personal financial information). Gli amministratori di rete possono, in modo semplice, analizzare, tracciare e intervenire in caso di violazione delle policy, e allo stesso tempo generare e fornire, ai propri dirigenti, relazioni dettagliate, per dimostrare in modo accurato lo stato dell'attività di DLP e gli sforzi, ad essa connessi, per far rispettare le disposizioni aziendali.

Estendere il valore

Il Web 2.0 ha spostato definitivamente l'obiettivo sostanziale della sicurezza Web; fornire protezione per i dati sensibili utilizzati all'interno del traffico Web è un aspetto che fa anch'esso ormai parte della sfida. Per le aziende che hanno scelto i nostri prodotti di sicurezza Web, tuttavia, raccogliere questa sfida non costituisce uno sforzo difficile e oneroso. È sufficiente implementare le funzionalità di sicurezza dei dati integrate che Websense mette a disposizione.

Tra i numerosi vantaggi, un approccio di questo tipo consente di:

- Favorire le attività aziendali in cui le tecnologie Web 2.0 sono necessarie, proteggendo gli utenti e i dati attraverso l'identificazione e la protezione da processi aziendali non autorizzati, errori involontari e codice dannoso in grado di rubare dati.
- Ottenere un maggiore livello di operatività, in particolare se comparato con soluzioni alternative che non permettono visibilità sull'identità e la destinazione, in caso di perdita di dati.
- Gestire e registrare non solo dove gli utenti stanno navigando sul web, funzionalità riscontrabile nella metà delle soluzioni di cui sei già in possesso, ma anche dove si stanno dirigendo i dati, per ragioni di compliance.
- Poter contare sulla qualità e sull'efficienza di una soluzione Websense, un'azienda che vanta esperienza e attestazioni di eccellenza senza confronti nel settore della sicurezza dei contenuti.

Non solo. Aiutando a risolvere quello che sta rapidamente diventando uno dei principali problemi per molte organizzazioni - il fornire una visibilità ampia e un controllo affidabile su dove i dati vengono inviati - aumenterà l'importanza e la credibilità del team dedicato alla sicurezza Web, dimostrando in modo chiaro il loro valore per il business.

E allora, cosa stai aspettando?